

Serial No. 10/723,450
Page 1 of 39

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

RECEIVED
CENTRAL FAX CENTER
SEP 23 2008

Patent Application

Inventor(s): Hung-Hsiang Jonathan Chao et al.
Case: Chao 1-77-1-14 (LCNT/126091)
Serial No.: 10/723,450 **Group Art Unit:** 2132
Filed: 11/26/2003 **Confirmation #:** 5965
Examiner: Kane, Cordelia P
Title: DISTRIBUTED ARCHITECTURE FOR STATISTICAL OVERLOAD
CONTROL AGAINST DISTRIBUTED DENIAL OF SERVICE
ATTACKS

CERTIFICATE OF MAILING OR TRANSMISSION
I hereby certify that this correspondence is being deposited with the
United States Postal Service with sufficient postage for first class
mail in an envelope addressed to: Commissioner for Patents, P.O.
Box 1450, Alexandria, VA 22313-1450, or being facsimile
transmitted to the USPTO, on the date indicated below.

09/23/2008

Y Morozova

Date

MAIL STOP APPEAL BRIEF-PATENTS
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

SIR:

APPEAL BRIEF

Appellants submit this Appeal Brief to the Board of Patent Appeals and Interferences on appeal from the decision of the Examiner of Group Art Unit 2132 mailed April 23, 2008 finally rejecting claims 1 – 12, 15, 18 – 21, 23, and 25 – 28.

In the event that an extension of time is required for this appeal brief to be considered timely, and a petition therefor does not otherwise accompany this appeal brief, any necessary extension of time is hereby petitioned for.

Appellants believe the only fee due is the \$510 Appeal Brief fee which is being charged to counsel's credit card. In the event Appellants are incorrect, the Commissioner is authorized to charge any other fees to Deposit Account No. 20-0782/LCNT/126091.

09/24/2008 HMARZ11 00000071 200782 10723450

01 FC:1402 510.00 DA

813014-1

Serial No. 10/723,450
Page 2 of 39

Table of Contents

1.	Identification Page.....	1
2.	Table of Contents	2
3.	Real Party in Interest	3
4.	Related Appeals and Interferences	4
5.	Status of Claims	5
6.	Status of Amendments	6
7.	Summary of Claimed Subject Matter	7
8.	Grounds of Rejection to be Reviewed on Appeal	14
9.	Arguments	15
10.	Conclusion	29
11.	Claims Appendix	30
12.	Evidence Appendix	38
13.	Related Proceedings Appendix	39

Serial No. 10/723,450
Page 3 of 39

Real Party in Interest

The real party in interest is LUCENT TECHNOLOGIES INC.

813014-1

Serial No. 10/723,450
Page 4 of 39

Related Appeals and Interferences

Appellants assert that no appeals or interferences are known to Appellants, Appellants' legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

813014-1

Serial No. 10/723,450
Page 5 of 39

Status of Claims

Claims 1 – 28 are pending in the application. Claims 1 – 28 were originally presented in the application. Claims 1 – 5, 8 – 11, 18, and 26 – 28 have been amended. Claims 13, 14, 16, 17, 22, and 24 are objected to. The final rejection of claims 1 – 12, 15, 18 – 21, 23, and 25 – 28 is appealed.

813014-1

Serial No. 10/723,450
Page 6 of 39

Status of Amendments

All claim amendments have been entered.

813014-1

Serial No. 10/723,450
Page 7 of 39

Summary of Claimed Subject Matter

Embodiments of the present invention are generally directed to prevention of distributed denial of service attacks in communication networks. More specifically, one embodiment of the present invention is directed to a method for selectively discarding packets during a distributed denial-of-service (DDoS) attack over a network. The network generally includes a centralized controller and a plurality of routers forming a security perimeter. The method includes aggregating victim destination prefix lists and attack statistics associated with incoming packets received from the plurality of security perimeter routers to confirm a DDoS attack victim. The method further includes aggregating packet attribute distribution frequencies for incoming victim related packets received from the plurality of security perimeter routers.

Further yet, the method includes generating common scorebooks based on the aggregated packet attribute distribution frequencies and nominal traffic profiles and aggregating local cumulative distribution function (CDF) of the local scores derived from the plurality of security perimeter routers. Also a common discarding threshold is derived from the CDF and sent to each of the plurality of security perimeter routers. The discarding threshold defines a condition in which an incoming packet may be discarded at the security perimeter.

For the convenience of the Board of Patent Appeals and Interferences, Appellants' independent claims 1, 8, 18, 26, 27 and 28 are presented below with citations to various figures and appropriate citations to at least one portion of the specification for elements of the appealed claims.

Claim 1 positively recites (with reference numerals, where applicable, and cites to at least one portion of the specification added):

1. (previously presented) A method for determining packets (202) to be discarded in response to a distributed denial-of-service (DDoS) attack, said method comprising:

813014-1

Serial No. 10/723,450
Page 8 of 39

confirming (224) a DDoS attack at a network location (110, 120) using a plurality of packet attribute values aggregated (222) from a plurality of routers (106) forming a security perimeter (114) of a network (100);

computing (242) an aggregate conditional probability measure for each packet (202) entering said location based on selected attributes (310, 316) included within said packet (202) from each of said plurality of security perimeter routers (106);

computing (248) an aggregate cumulative distribution function (CDF) of scores based on said computed aggregate conditional probability measures;

determining (246) a discarding threshold using said cumulative probability function; and

sending (249) said discarding threshold to each of said plurality of security perimeter routers (104).

Support for the elements of claim 1 can be found at least from the following sections of Appellants' specification: page 2, line 26 –page 3, line 9; page 3, line 30 – page 4, line 26; page 5, line 16 – page 6, line 16; page 6, line 29 – page 7, line 27; page 8, line 4 – page 9, line 3; page 11, lines 25 – 30; page 12, lines 5 – 19; page 12, line 30 – page 14, line 24; page 15, line 18 – page 16, line 6; page 16, line 22 – page 17, line 15; page 18, lines 9 – 16; page 19, lines 7 – 22; page 20, line 6 – page 21, line 11; page 24, lines 10 – 14; page 25, line 24 – page 26, line 5; page 26, line 18 – page 28, line 22; and Figs. 1 – 3.

Claim 8 positively recites (with reference numerals, where applicable, and cites to at least one portion of the specification added):

8. (previously presented) A method for selectively discarding packets (202) during a distributed denial-of-service (DDoS) attack over a network (100), comprising:

aggregating (222), in said network (100) comprising a centralized controller (108) and a plurality of routers (106) forming a security perimeter (114), victim destination prefix lists and attack statistics (310, 316) associated with incoming packets (202)

813014-1

Serial No. 10/723,450
Page 9 of 39

received from said plurality of security perimeter routers (106) to confirm (224) a DDoS attack victim (120);

aggregating (242) packet attribute distribution frequencies for incoming victim related packets (202) received from said plurality of security perimeter routers (106);

generating (244) common scorebooks from said aggregated (242) packet attribute distribution frequencies and nominal traffic profiles (241);

aggregating (248) local cumulative distribution function (CDF) of local scores derived (245) from said plurality of security perimeter routers (106); and

providing (249), to each of said plurality of security perimeter routers (106), a common discarding threshold, said discarding threshold defining a condition in which an incoming packet (202) may be discarded at said security perimeter (114).

Support for the elements of claim 8 can be found at least from the following sections of Appellants' specification: page 2, line 26 –page 3, line 9; page 3, line 30 – page 4, line 26; page 5, line 16 – page 6, line 16; page 6, line 29 – page 7, line 27; page 8, line 4 – page 9, line 3; page 9, line 23 – page 10, line 9; page 11, lines 25 – 30; page 12, lines 5 – 19; page 12, line 30 – page 14, line 24; page 15, line 18 – page 16, line 6; page 16, line 22 – page 17, line 15; page 18, lines 9 – 16; page 19, lines 7 – 22; page 20, line 6 – page 21, line 11; page 24, lines 10 – 14; page 25, line 24 – page 26, line 5; page 26, line 18 – page 28, line 22; and Figs. 1 – 3.

Claim 18 positively recites (with reference numerals, where applicable, and cites to at least one portion of the specification added):

18. (previously presented) A method for selectively discarding packets (202) at a security perimeter (114) of a network (100) during a distributed denial-of-service (DDoS) attack over said network (100), comprising:

sending (211), from each of a plurality of routers (106) forming said security perimeter (114), victim destination prefix list and attack statistics (310, 316) associated with incoming packets (202) to a centralized controller (108) adapted to confirm (224) a victim (120) of said DDoS attack;

813014-1

Serial No. 10/723,450
Page 10 of 39

sending (233), from each of said plurality of security perimeter routers (106), packet attribute distribution frequencies for incoming victim related packets (202);

receiving (245), at each of said plurality of security perimeter routers (106) from said centralized controller (108), common scorebooks formed (244) using aggregated (242) packet attribute distribution frequencies and nominal traffic profiles (241);

sending (247), from each of said plurality of security perimeter routers (106), a local cumulative distribution function (CDF) of scores to said centralized controller (108); and

discarding (250), at each of said plurality of security perimeter routers (106), incoming packets (202) based on a commonly distributed discarding threshold defined by said centralized controller (108).

Support for the elements of claim 18 can be found at least from the following sections of Appellants' specification: page 2, line 26 – page 3, line 9; page 3, line 30 – page 4, line 26; page 5, line 16 – page 6, line 16; page 6, line 29 – page 7, line 27; page 8, line 4 – page 9, line 3; page 9, line 23 – page 10, line 9; page 11, lines 25 – 30; page 12, lines 5 – 19; page 12, line 30 – page 14, line 24; page 15, line 18 – page 16, line 6; page 16, line 22 – page 17, line 15; page 18, lines 9 – 16; page 19, lines 7 – 22; page 20, line 6 – page 21, line 11; page 24, lines 10 – 14; page 25, line 24 – page 26, line 5; page 26, line 18 – page 28, line 22; and Figs. 1 – 3.

Claim 26 positively recites (with reference numerals, where applicable, and cites to at least one portion of the specification added):

26. (previously presented) A centralized controller (108) for determining packets (202) to be dropped in regard to a potential distributed denial-of-service (DDoS) attack at a location within a packet network (100), said centralized controller (108) comprising:

means (108) for aggregating (222) a plurality of packet attribute values respectively received (211) from a plurality routers (106) forming a security perimeter (114) of a network (100) to confirm (224) said attack at said

813014-1

Serial No. 10/723,450
Page 11 of 39

location, wherein said centralized controller (108) is associated with said network (100);

means (108) for computing (242) an aggregate conditional probability measure for each packet (202) entering said location based on selected attributes (310) included within said packet (202) from each location;

means (108) for computing (248) an aggregate cumulative distribution function (CDF) based on said computed aggregate conditional probability measures;

means (108) for determining (246) a drop threshold based on access to said cumulative probability function; and

means (108) for sending (249) said drop threshold to each of said plurality of security perimeter routers (106), wherein each of said plurality of security perimeter routers (106) is adapted to pass through packets (202), that exceed said determined drop threshold, to said location.

Support for the elements of claim 26 can be found at least from the following sections of Appellants' specification: page 2, line 26 – page 3, line 9; page 3, line 30 – page 4, line 26; page 5, line 16 – page 6, line 16; page 6, line 29 – page 7, line 27; page 8, line 4 – page 9, line 3; page 9, line 23 – page 10, line 9; page 11, lines 25 – 30; page 12, lines 5 – 19; page 12, line 30 – page 14, line 24; page 15, line 18 – page 16, line 6; page 16, line 22 – page 17, line 15; page 18, lines 9 – 16; page 19, lines 7 – 22; page 20, line 6 – page 21, line 11; page 24, lines 10 – 14; page 25, line 24 – page 26, line 5; page 26, line 18 – page 28, line 22; and Figs. 1 – 3.

Claim 27 positively recites (with reference numerals, where applicable, and cites to at least one portion of the specification added):

27. (previously presented) A centralized controller (108) for determining packets (202) to be dropped in regard to a potential distributed denial-of-service (DDoS) attack at a location within a packet network (100), said centralized controller (108) comprising:

813014-1

Serial No. 10/723,450
Page 12 of 39

means (108) for aggregating (222), local victim destination prefix lists and attack statistics (310, 316) associated with incoming packets (202) received from a plurality of routers (106) of a network (100) forming a security perimeter (114) in said network (100), to confirm a victim (120) of said DDoS attack, wherein said centralized controller (108) is associated with said network (100);

means (108) for aggregating (222) packet attribute distribution frequencies for incoming victim related packets (202) received from said plurality of security perimeter routers (106);

means (108) for generating (244) common scorebooks from said aggregated (242) packet attribute distribution frequencies and nominal traffic profiles (241);

means (108) for aggregating (248) local cumulative distribution function (CDF) of the local scores derived (247) from said plurality of security perimeter routers (106); and

means (108) for providing (249), to each of said plurality of security perimeter routers (106), a common discarding threshold, said discarding threshold defining a condition in which an incoming packet (202) may be discarded at said security perimeter (114).

Support for the elements of claim 27 can be found at least from the following sections of Appellants' specification: page 2, line 26 – page 3, line 9; page 3, line 30 – page 4, line 26; page 5, line 16 – page 6, line 16; page 6, line 29 – page 7, line 27; page 8, line 4 – page 9, line 3; page 9, line 23 – page 10, line 9; page 11, lines 25 – 30; page 12, lines 5 – 19; page 12, line 30 – page 14, line 24; page 15, line 18 – page 16, line 6; page 16, line 22 – page 17, line 15; page 18, lines 9 – 16; page 19, lines 7 – 22; page 20, line 6 – page 21, line 11; page 24, lines 10 – 14; page 25, line 24 – page 26, line 5; page 26, line 18 – page 28, line 22; and Figs. 1 – 3.

Claim 28 positively recites (with reference numerals, where applicable, and cites to at least one portion of the specification added):

813014-1

Serial No. 10/723,450
Page 13 of 39

28. (previously presented) A network (100) comprising:
a centralized controller (108) for determining packets (202) to be dropped in regard to a potential distributed denial-of-service (DDoS) attack at a location within a packet network (100); and
a plurality of security perimeter routers (106) wherein each of said security perimeter routers (106) comprises:
means (106, 116) for sending (211) victim destination prefix lists and attack statistics (310, 316) associated with incoming packets (202) to said centralized controller (108) adapted to confirm a victim of said DDoS attack;
means (106, 116) for sending (233) to said centralized controller (108) packet attribute distribution frequencies for incoming victim related packets;
means (106, 116) for receiving (245), from said centralized controller (108), common scorebooks formed by aggregated (242) packet attribute distribution frequencies and nominal traffic profiles (241);
means (106, 116) for sending (247) a local cumulative distribution function (CDF) of scores to said centralized controller (108); and
means (106, 116) for discarding incoming packets (202) based on a commonly distributed, to said plurality of security perimeter routers (106), discarding threshold defined by said centralized controller (108).

Support for the elements of claim 28 can be found at least from the following sections of Appellants' specification: page 2, line 26 –page 3, line 9; page 3, line 30 – page 4, line 26; page 5, line 16 – page 6, line 16; page 6, line 29 – page 7, line 27; page 8, line 4 – page 9, line 3; page 9, line 23 – page 10, line 9; page 11, lines 25 – 30; page 12, lines 5 – 19; page 12, line 30 – page 14, line 24; page 15, line 18 – page 16, line 6; page 16, line 22 – page 17, line 15; page 18, lines 9 – 16; page 19, lines 7 – 22; page 20, line 6 – page 21, line 11; page 24, lines 10 – 14; page 25, line 24 – page 26, line 5; page 26, line 18 – page 28, line 22; and Figs. 1 – 3.

813014-1

Serial No. 10/723,450
Page 14 of 39

Grounds of Rejection to be Reviewed on Appeal

Claims 1, 3, 8 – 12, 15, 18 – 21, 23, and 25 – 28 are rejected under 35 U.S.C. §102(e) as being anticipated by Chesla et al.'s U.S. Publication 2004/0250124 A1 (hereinafter "Chesla").

Claims 1 – 7 and 26 are rejected under 35 U.S.C. §102(e) as being anticipated by Lau et al.'s US Publication 2004/0062199 A1 (hereinafter "Lau").

813014-1

Serial No. 10/723,450
Page 15 of 39

Arguments

Rejections Under 35 U.S.C. §102

Claims 1, 3, 8 – 12, 15, 18 – 21, 23, and 25 – 28

Claims 1, 3, 8 – 12, 15, 18 – 21, 23, and 25 – 28 are rejected under 35 U.S.C. §102(e) as being anticipated by Chesla. The rejection is traversed.

The Applicable Law

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

"To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999); *see also* MPEP § 2112.

The Reference

In general, Chesla is directed to an apparatus and a method for protecting networks against malicious traffic, including against distributed denial-of-service (DDoS) network flood attacks. More specifically, Chesla describes a network security system that detects and filters traffic entering a protected network. The security system uses adaptive fuzzy logic algorithms to analyze traffic patterns in real-time to detect anomalous traffic patterns indicative of an attack. Upon detection of an attack, the security system determines parameters of the anomalous traffic and then filters future traffic using these parameters. The security system also monitors efficiency of the performed filtering and adjusts filtering rules to optimize blocking of malicious traffic

813014-1

Serial No. 10/723,450
Page 16 of 39

and minimize blocking of legitimate traffic. The security system is typically implemented as a network appliance deployed on the perimeter of the protected network and may be located outside a firewall of the network (see Chesla, paragraphs [0001], [0016] – [0020]).

The Examiner's Arguments

1. The Examiner asserts that Fig. 1C of Chesla teaches “a plurality of routers forming a security perimeter of a network,” as recited in Appellants’ claim 1. More specifically, relying on paragraph [0118], the Examiner argues that Chesla discloses multiple routers and that such routers constitute the security system, which is deployed at the periphery of the network (see Advisory Action, page 2).
2. The Examiner asserts that Chesla teaches “determining a discarding threshold using said cumulative probability function,” as recited in Appellants’ claim 1, because in paragraph [0135] “Chesla teaches that the packets are filtered based on the threshold collected from trapping module which is based on information received from the FIS module” (see Advisory Action, page 2).
3. The Examiner asserts that Chesla teaches “confirming a DDoS attack in a network location using a plurality of packet attribute values aggregated from a plurality of security perimeter routers” in Fig. 1C and paragraphs [0118] and [0376] (see Final Office Action, page 3).
4. The Examiner asserts that Chesla teaches “sending said discarding threshold to each of said plurality of security perimeters” in paragraph [0323]. More specifically, the Examiner reasons that “[s]ince the filtering would be in the routers then the information computed in the FIS module would have to be passed to the filters/routers, to be able to filter” (see Final Office Action, page 3).
5. The Examiner asserts that Chesla teaches “aggregating, in said network comprising a centralized controller and a plurality of routers forming a security perimeter, victim destination prefix lists and attack statistics associated with incoming packets received from said plurality of security

813014-1

Serial No. 10/723,450
Page 17 of 39

perimeter routers to confirm a DDoS attack victim,” as recited in independent claim 8. More specifically, the Examiner cites Fig. 1 and paragraphs [0118], [0224], and [0376] and reasons that “since each potential victim would have the same prefix since it is on the same customer network, the aggregating of the statistics will also be an aggregation of the victim prefix list” (see Final Office Action, pages 3 – 4).

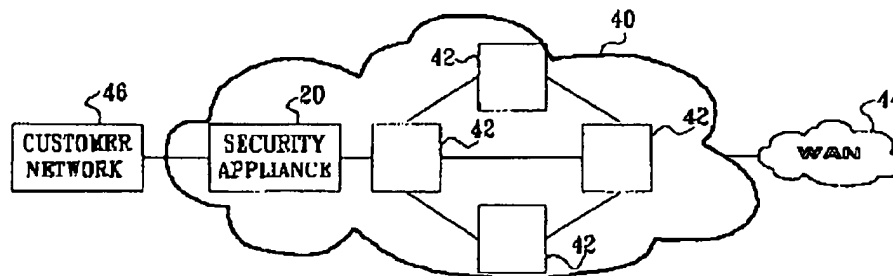
Appellants’ Response to the Examiner’s Arguments

1. Chesla fails to teach or suggest at least “a plurality of routers forming a security perimeter of a network,” as recited in independent claim 1.

For the convenience of the Board, paragraph [0118] and Fig. 1C of Chesla are provided below. Paragraph [0118] of Chesla states:

“FIG. 1C is a block diagram that schematically illustrates network security system 20 deployed at the periphery of an Internet Service Provider (ISP) facility 40, in accordance with an embodiment of the present invention. The ISP facility typically comprises various network elements 42, such as routers, switches, bridges, servers, and clients. ISP 40 is connected to at least one WAN 44, typically the Internet, and many customer networks, such as a customer network 46. ISP 40 typically deploys security system 20 between the periphery of the ISP facility and customer network 46. The ISP may, for example, offer customers the security protection provided by system 20 as a managed service” (emphasis added).

FIG. 1C



813014-1

Serial No. 10/723,450
Page 18 of 39

The Examiner asserts that the above shown Fig. 1C and recited paragraph [0118] disclose multiple routers constituting a security system deployed at the periphery of a network (see Advisory Action, page 2). However, the only plurality of routers that are discussed in paragraph [0018] are network elements 42. Such network elements with other network elements form the ISP facility 40, which in turn deploys the security system 20 between the periphery of the ISP facility 40 and the customer network 46.

Though Appellants have repeatedly indicated that Appellants are not clear as to which element in Figure 1C the Examiner interprets as the network of Appellants' claim 1, namely the ISP 40 (option 1) or the customer network 46 (option 2), the Examiner has not clarified this issue yet. However, with either interpretation, the network elements 42 cannot be equated to the Appellants' security perimeter routers.

Option 1:

Paragraph [0118] does not state that the network elements 42 are located at the perimeter of the ISP, instead they are described as being included in the ISP, and thus, do not necessarily form the perimeter of the ISP. Only the security system 20 is described as being possibly deployed at the periphery of the ISP. The Examiner states that the routers work with the network appliance (security system), and thus, are part of the security system. According to such a rationale, the customer network, which also works with the network appliance, may be considered as a part of the security system. However, this clearly contradicts the Chesla arrangements because the security system serves to protect multiple customer networks.

Furthermore, following the Examiner's rationale and considering Appellants' claim 1 as a whole, if the network elements 42 form the security perimeter of the ISP, then DDoS attacks should be directed at a location within the ISP. However, this also contradicts the Chesla arrangement because the ISP serves to protect the customer network from attacks and such attacks are directed to locations within the customer network. The network elements 42 do not protect the ISP from the attacks.

Serial No. 10/723,450
Page 19 of 39

Option 2:

In paragraph [0118], Chesla discusses two possible locations for the network appliance (security system), namely at the periphery of the ISP 40 or between the periphery of the ISP 40 and customer network 46. However, in either case, the security system 20 is between the network elements 42 and the customer network 46. Accordingly, the security system 20 placement prevents the network elements 42 from forming a security perimeter of the customer network 46.

Furthermore, as described by Chesla, one ISP connects WAN to multiple customer networks. Therefore, as described by Chesla, there is only one point of connection between the multiple customer networks and multiple network elements, namely the network appliance (security system 20). Accordingly, even assuming that the network elements 42 are part of the security system 20 and the security system is at the perimeter of one of the customer networks, because there is only one point of connection between the network elements 20 and the customer networks, the network elements 42 at most may be considered as one element of the perimeter, and thus, at most be equated to only one router of Appellants' claim 1.

Accordingly, under either interpretation, Chesla does not teach or suggest at least a plurality of routers forming a security perimeter of a network.

2. Additionally, Chesla fails to teach or suggest at least: "determining a discarding threshold using said cumulative probability function," as recited in Appellants' claim 1.

Paragraph [0135] of Chesla states:

"[I]f the anomaly is not transient, filtering module 70 filters incoming traffic, at a filtering step 110, using the signatures determined by trapping module 68 at step 106 ... When the counter is at its initial, lowest level, the filtering module uses a relatively narrow set of signatures, in order to minimize the likelihood of blocking legitimate traffic (i.e., false positives). As the counter is incremented ... the intensity of filtering provided by the signatures is gradually increased ... If the FIS module determines that the attack is continuing despite the filtering, the controller determines whether the attack level has changed ... A change in the attack level (negative feedback) is interpreted either as an indication that the nature of the attack has changed, or as an indication that a second, independent attack has

Serial No. 10/723,450

Page 20 of 39

begun in addition to the attack already detected. In either case, the method returns to step 106 for new trapping to address the new attack or the modified old attack, as the case may be” (emphasis added).

In sum, paragraph [0135] of Chesla describes using signatures to filter traffic and adjusting such signatures when filtering is inefficient. It appears that the Examiner equates signatures of Chesla with Appellants’ discarding threshold. Appellants respectfully disagree with such an interpretation.

In general, a signature describes a pattern of an attack or security violation (see Chesla, paragraphs [0008] – [0010]). More specifically, in Chesla the signatures represent values of one or more packet header fields or information from the packet payload, e.g., a UDP DNS query string (see Chesla, paragraph [0023]). Such signatures are compared to incoming packets and matching packets are discarded. In contrast, an ordinary meaning of the term “threshold” is a point of beginning, such as a minimum/maximum requirement for further action. Because the signatures of Chesla are used only to find a match, each of such signatures cannot be considered a threshold.

Furthermore, paragraph [0135] is silent with respect to “using said cumulative probability function.” In the final Office Action, the Examiner has relied on paragraph [0225] of Chesla as disclosing this limitation.

Paragraph [0225] states:

“... The FIS module defuzzifies this fuzzy set, i.e., resolves the fuzzy set into a single value representing a degree of the attack, at a defuzzification step 296. For example, the degree of attack may have a range between 2 and 10, with higher numbers indicative of a greater likelihood that an attack is occurring. A degree of attack value between 2 and 4 may represent a normal (non-attack) degree, a value between 4 and 8 may represent a suspect (potential) attack degree, and a value between 8 and 10 may represent an attack degree. The FIS module passes the degree of attack to network flood controller 60, at [a] degree of attack output step 298. The controller typically interprets the output as an indication of the occurrence of an attack when the degree of attack exceeds a certain threshold, e.g., 8 out of a range between 2 and 10” (emphasis added).

However, paragraph [0225] does not discuss how signatures are determined or even mention signatures. Rather, paragraph [0225] describes possible degrees of an attack. Accordingly, even assuming *arguendo* that Chesla’s signature may be considered

813014-1

Serial No. 10/723,450
Page 21 of 39

to be a threshold, Chesla still fails to teach or suggest determining such a signature using a cumulative probability function.

Moreover, the threshold discussed in paragraph [0225] cannot be equated with Appellants' threshold either. More specifically, Chesla states that "8" might be a value of the threshold defining that an attack has occurred. However, the threshold defining an attack degree is simply not the same as Appellants' discarding threshold. As Chesla describes in paragraphs [0132] through [0134], even when a determined attack degree is above the threshold, i.e., "8," network packets are not necessarily discarded. For example, if after recognizing an attack degree above "8" it is determined that the attack was transient, no traffic is discarded. In contrast, the Appellants' discarding threshold defines a condition in which an incoming packet should be discarded at the security perimeter.

Furthermore, Chesla's threshold is pre-defined as a number between 2 and 10. In contrast, Appellants' discarding threshold is not pre-defined, rather it is determined, using for example, cumulative probability function. Accordingly, Chesla does not teach or suggest "determining a discarding threshold using said cumulative probability function," as recited in Appellants' claim 1.

3. Chesla fails to teach or suggest "confirming a DDoS attack in a network location using a plurality of packet attribute values aggregated from a plurality of security perimeter routers," as recited in independent claim 1.

First, as discussed above, Chesla does not teach a plurality of security routers. Consequently, Chesla simply cannot teach or suggest "using a plurality of packet attribute values aggregated from a plurality of security perimeter routers." Second, even assuming *arguendo* that Chesla suggests a plurality of security perimeter routers, paragraphs [0118] and [0376] do not teach or suggest packet attribute values being aggregated from the plurality of the security perimeter routers. Chesla does not mention such a process of aggregation and it is not necessary. For example, each security perimeter router may confirm a DDoS attack using only packet attribute values of packets received at such a router. Therefore, Chesla does not teach or suggest "confirming a

Serial No. 10/723,450
Page 22 of 39

DDoS attack in a network location using a plurality of packet attribute values aggregated from a plurality of security perimeter routers,” as recited in Appellants’ claim 1.

4. Chesla fails to teach or suggest “sending said discarding threshold to each of said plurality of security perimeters,” as recited in independent claim 1.

First, as discussed above, Chesla does not teach or suggest a plurality of security perimeter routers. Consequently, Chesla simply cannot teach or suggest “sending said discarding threshold to each of said plurality of security perimeter routers.” Second, as also discussed above, Chesla does not teach or suggest a discarding threshold. Consequently, Chesla simply cannot teach or suggest “sending said discarding threshold to each of said plurality of security perimeter routers.”

Finally, assuming *arguendo* that Chesla teaches the plurality of security perimeter routers and discarding threshold, Chesla still fails to teach or suggest “sending said discarding threshold to each of said plurality of security perimeter routers.” Nowhere does Chesla disclose such an action explicitly. Furthermore, it is not inherent from Chesla that each of these routers would receive a discarding threshold, or that all of these routers would receive the same discarding threshold. For example, a security perimeter router may calculate a discarding threshold on its own or, respectively, two security perimeter routers may receive different discarding thresholds. Accordingly, because arrangements, other than ones suggested by the Examiner, are possible in the context Chesla, Appellants’ limitation of “sending said discarding threshold to each of said plurality of security perimeter routers” is not inherent from Chesla.

5. Chesla fails to teach or suggest “aggregating, in said network comprising a centralized controller and a plurality of routers forming a security perimeter, victim destination prefix lists and attack statistics associated with incoming packets received from said plurality of security perimeter routers to confirm a DDoS attack victim,” as recited in independent claim 8.

First, as discussed above, Chesla does not teach or suggest a plurality of security perimeter routers. Consequently, Chesla simply cannot teach or suggest “aggregating ... victim destination prefix lists and attack statistics ... received from said plurality of

813014-1

Serial No. 10/723,450
Page 23 of 39

security perimeter routers.” Second, even assuming *arguendo* that Chesla suggests a plurality of security perimeter routers, paragraphs [0118], [0224], and [0376] do not teach or suggest aggregating data from the plurality of the security perimeter routers. The cited portions of Chesla do not mention such a process of aggregation from multiple routers and it is not necessary for the Chesla arrangement to function as intended. For example, victim destination prefix lists and attack statistics data may be aggregated and analyzed independently at each of security perimeter routers.

Third, the Examiner appears to suggest that aggregating victim destination prefix lists is inherent from Chesla. More specifically, the Examiner reasons that “since each potential victim would have the same prefix since it is on the same customer network, the aggregating of the statistics will also be an aggregation of the victim prefix list.” However, Chesla describes ISP 40 as being connected to “many customer networks, such as customer network 46.” Accordingly, contrary to the Examiner’s suggestion, aggregated statistics may include statistics from multiple customer networks.

Furthermore, because Chesla does not disclose aggregating all possible types of information with respect to the incoming packets, the victim prefix information may simply be identified, but not collected. Because aggregation requires that the information not only be received, but also collected, and because collection of the victim destination prefix is not necessary for the Chesla arrangement to function as intended, Chesla does not teach or suggest aggregating victim destination prefix lists. Accordingly, Chesla does not teach or suggest the above recited element of Appellants’ claim 8.

Conclusion

Accordingly, for the reasons discussed with respect to points 1 – 4, Chesla does not teach or suggest each and every element of Appellants’ claim 1. As such, independent claim 1 is not anticipated by Chesla and is allowable under 35 U.S.C. §102. Independent claims 8, 18, 26, and 27 recite at least some limitations that are similar to those recited in independent claim 1 and discussed above. Accordingly, at least for the same reasons as discussed above, these independent claims also are not anticipated by Chesla and are allowable under 35 U.S.C. §102.

813014-1

Serial No. 10/723,450
Page 24 of 39

Furthermore, numerous elements of independent claims 8, 18, 26, and 27 recite the plurality of security perimeter routers. Because, as discussed above, Chesla does not disclose the plurality of security perimeter routers, each such element is not anticipated by Chesla.

Chesla also does not teach or suggest each and every element of Appellants' claims 8, 18, 26, and 27 for the reasons discussed with respect to point 5, where claims 18, 26, and 27 recite limitations similar to the discussed limitations of claim 8. Accordingly, at least for the reasons discussed above, these independent claims are not anticipated by Chesla and are allowable under 35 U.S.C. §102.

Moreover, because all of the dependent claims that depend from the independent claims include all the limitations of the respective independent claim from which they ultimately depend, each such dependent claim is also allowable.

Therefore, Appellants' claims 1, 3, 8 – 12, 15, 18 – 21, 23, and 25 – 28 are allowable under 35 U.S.C. §102(e), and thus, the rejection should be withdrawn.

Claims 1 – 7 and 26

Claims 1 – 7 and 26 are rejected under 35 U.S.C. §102(e) as being anticipated by Lau. The rejection is traversed.

The Applicable Law

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

"To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result

813014-1

Serial No. 10/723,450
Page 25 of 39

from a given set of circumstances is not sufficient." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999); *see also* MPEP § 2112.

The Reference

In general, Lau is directed to an apparatus and a method for an overload control procedure against denial of service attack. More specifically, Lau discloses a method where an incoming packet is prioritized based on conditional probability of attributes carried by the packet. The conditional probability of each packet is evaluated by comparing the attributes carried by an incoming packet against the "nominal" distribution of attributes of legitimate packet stream. To provide an online one-pass selectively dropping scheme, a cumulative distribution function (CDF) of the conditional legitimate probability of all incoming packets is maintained and a threshold-based selective based mechanism is applied to each incoming packet according to the conditional probability value calculated for that packet. In one embodiment of Lau, the method is implemented at a network processor for protecting a network server from an overload of IP packets sent from a router (see e.g., Lau, paragraphs [0004], [0015]).

The Examiner's Arguments

1. The Examiner asserts that Lau teaches "a plurality of packet attribute values aggregated from a plurality of routers forming a security perimeter of a network," as recited in independent claim 1. More specifically, the Examiner suggests that paragraph [0015] of Lau teaches "a plurality of routers that are feeding data into the network ... and are therefor on the perimeter of the network." The Examiner reasons that "these routers and network processors perform the filtering and therefor create a security perimeter." The Examiner further indicates that because Lau teaches aggregating packet attribute values all limitations of the above recited element of Appellants' claim 1 are taught by Lau (see Advisory Action, page 2).
2. The Examiner asserts that Lau teaches "sending said discarding threshold to each of said plurality of security perimeter routers" in paragraph [0016]. More specifically, the Examiner reasons that "[s]ince there may be multiple

813014-1

Serial No. 10/723,450
Page 26 of 39

routers or NPs then the information need to be distributed” (see Final Office Action, page 10).

Appellants' Response to the Examiner's Arguments

1. Lau does not teach or suggest at least “a plurality of packet attribute values aggregated from a plurality of routers forming a security perimeter of a network,” as recited in independent claim 1.

Paragraph [0015] of Lau states:

“In an exemplary embodiment of the present invention, a network processor (NP) is used to protect a network server from an overload of IP packets sent from a router. Referring now to FIG. 1, a NP 30 is shown within network 10. The network 10 also comprises at least one router 20 and at least one server 40. The NP 30 is adapted to detect and filter IP packets traveling, for example, from the router 20 to the server 40. IP packets come in various forms including email, file transfers, and ping/UDP/ICMP floods. Those skilled in the art will appreciate that NPs are generally capable of processing IP packets as fast as they can receive them at OC3 or above rates (i.e., at a rate of hundreds of thousands of packets per second)” (emphasis added).

Nowhere in the cited portion does Lau disclose that the network processor, router, or their combination form a perimeter router. In contrast, Lau explicitly states that a network processor protects a network server from overload packets sent from a router. Accordingly, even if such a router “feed[s] data into the network,” Lau’s router simply cannot be equated with the Appellants’ security perimeter router because Lau’s router actually causes the overload packets to be transmitted to the network server while Appellants’ security perimeter router discards offensive packets.

With respect to the network processor, the Lau disclosure and paragraph [0015] in particular discuss only a single network processor per a network server. In contrast Appellants claim a plurality of routers forming a security of the network.

Furthermore, even assuming *arguendo* that Lau suggests that there may be a plurality of the network processors and such network processors would form a security perimeter of the network, Lau does not teach or suggest packet attribute values being aggregated from the plurality of the network processors. In other words, Lau does not teach or suggest a packet attribute value of a packet received at one network processor of the plurality of network processors being aggregated with a packet attribute value of

813014-1

Serial No. 10/723,450
Page 27 of 39

another packet received at another network processor of the plurality of the network processors. Rather, the exemplary embodiment of Lau includes only one server, one network processor, and one router, and merely mentions that additional units may be used. Consequently, Lau does not discuss aggregation of packet attributes values from a plurality of network processors.

Furthermore, aggregating packet attribute values from such a plurality of network processors is not inherent from Lau because an alternative arrangement is possible in the context of the Lau disclosure. For example, each network processor may aggregate values of only packets passing through that particular network processor. Therefore, Lau does not teach or suggest at least “a plurality of packet attribute values aggregated from a plurality of routers forming a security perimeter of a network.”

2. Lau also does not teach or suggest at least “sending said discarding threshold to each of said plurality of security perimeter routers,” as recited in independent claim 1.

First, as discussed above, Lau does not teach a plurality of security perimeter routers. Rather, in paragraph [0016], Lau merely mentions “that although server 40, NP [network processor] 30 and router 20 have been depicted as three units in FIG. 1, they may comprise fewer or additional units,” where the server, NP, and router form a network 10. Because, an additional unit is not necessarily NP or a router, but rather any network element, plurality of security perimeter routers is not inherent from Lau.

Second, assuming *arguendo* that Lau teaches a plurality of security perimeter routers, it is not inherent from Lau that each of these routers would receive a discarding threshold, or that all of these routers would receive the same discarding threshold. For example, a security perimeter router may calculate a discarding threshold on its own or, respectively, two security perimeter routers may receive different discarding thresholds. Accordingly, because arrangements, other than ones suggested by the Examiner, are possible in the context Lau, “sending said discarding threshold to each of said plurality of security perimeter routers,” is not inherent from Lau.

Serial No. 10/723,450
Page 28 of 39

Conclusion

Therefore, as discussed above with respect to points 1 and 2, Lau fails to disclose each and every element of the claimed invention, as arranged in Appellants' independent claim 1. As such, independent claim 1 is not anticipated by Lau and is allowable under 35 U.S.C. §102. Because claims 2 – 6 depend from independent claim 1, and thus, include all the elements of claim 1, each such dependent claim is also allowable over Lau. Independent claim 26 recites limitations similar to those recited in independent claim 1 and, as such, and at least for the same reasons as discussed above, independent claim 26 also is not anticipated by Lau and is allowable under 35 U.S.C. §102.

Therefore, Appellants' claims 1 – 7 and 26 are allowable under 35 U.S.C. §102(e), and thus, the rejection should be withdrawn.

813014-1

Serial No. 10/723,450
Page 29 of 39

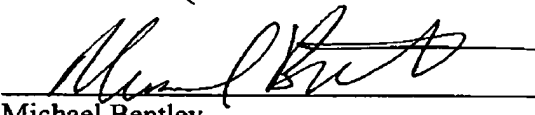
Conclusion

Thus, Appellants submit that all of the claims presently in the application are allowable.

For the reasons advanced above, Appellants respectfully urge that the rejection of claims 1-12, 15, 18-21, 23 and 25-28 is improper. Reversal of the rejections of the Final Office Action is respectfully requested.

Respectfully submitted,

Dated: 9/22/08



Michael Bentley
Registration No. 52,613
Patterson & Sheridan, L.L.P.
595 Shrewsbury Ave. Suite 100
Shrewsbury, NJ 07702
Telephone: (732) 530-9404
Facsimile: (732) 530-9808
Agent for Appellants

Serial No. 10/723,450

Page 30 of 39

CLAIMS APPENDIX

1. (previously presented) A method for determining packets to be discarded in response to a distributed denial-of-service (DDoS) attack, said method comprising:

confirming a DDoS attack at a network location using a plurality of packet attribute values aggregated from a plurality of routers forming a security perimeter of a network;

computing an aggregate conditional probability measure for each packet entering said location based on selected attributes included within said packet from each of said plurality of security perimeter routers;

computing an aggregate cumulative distribution function (CDF) of scores based on said computed aggregate conditional probability measures;

determining a discarding threshold using said cumulative probability function; and

sending said discarding threshold to each of said plurality of security perimeter routers.

2. (previously presented) The method of claim 1, wherein said step of computing an aggregate conditional probability measure further comprises:

updating an individual marginal probability mass function and a joint probability mass function for attributes carried by each said packet.

3. (previously presented) The method of claim 1, further comprising:

granting immunity to packets of a specified sub-type entering said location.

4. (previously presented) The method of claim 1, wherein said aggregate conditional probability measure is computed in accordance with the following equation:

$$CP(p) = \frac{\rho_n}{\rho_m} \cdot \frac{JP_n(A = a_p, B = b_p, C = c_p, \dots)}{JP_m(A = a_p, B = b_p, C = c_p, \dots)}$$

where: ρ_m is currently measured utilization of a system;

ρ_n is nominal utilization of the system;

813014-1

Serial No. 10/723,450
Page 31 of 39

A, B, C, \dots is a set of packet attributes;

$JP_n(A, B, C, \dots)$ is a joint probability mass function of the set of attributes under normal traffic conditions;

$JP_m(A, B, C, \dots)$ is the joint probability mass function of the set of attributes measured under current traffic conditions; and

a, b, c, \dots are the particular values that the attributes A, B, C, \dots take.

5. (previously presented) The method of claim 1, wherein said aggregate conditional probability measure is computed in accordance with the following equation:

$$CP(p) = \frac{\rho_n}{\rho_m} \cdot \frac{P_n(A = a_p)}{P_m(A = a_p)} \cdot \frac{P_n(B = b_p)}{P_m(B = b_p)} \cdot \frac{P_n(C = c_p)}{P_m(C = c_p)}$$

where: ρ_m is currently measured utilization of a system;

ρ_n is nominal utilization of the system;

$A, B,$ and C is a set of packet attributes;

$P_n(A, B, C)$ is a marginal probability mass function of the set of attributes under normal traffic conditions;

$P_m(A, B, C)$ is the marginal probability mass function of the set of attributes measured under current traffic conditions; and

$a, b,$ and $c,$ are the particular values that the attributes $A, B,$ and C take.

6. (original) The method of claim 1, wherein said discarding threshold is calculated using a load shedding algorithm, combined with an inverse lookup on the aggregate CDF of scores.

7. (original) The method of claim 2, wherein said joint and marginal probability functions are maintained using iceberg-style histograms.

8. (previously presented) A method for selectively discarding packets during a distributed denial-of-service (DDoS) attack over a network, comprising:

aggregating, in said network comprising a centralized controller and a plurality of routers forming a security perimeter, victim destination prefix lists and attack statistics

813014-1

Serial No. 10/723,450
Page 32 of 39

associated with incoming packets received from said plurality of security perimeter routers to confirm a DDoS attack victim;

aggregating packet attribute distribution frequencies for incoming victim related packets received from said plurality of security perimeter routers;

generating common scorebooks from said aggregated packet attribute distribution frequencies and nominal traffic profiles;

aggregating local cumulative distribution function (CDF) of local scores derived from said plurality of security perimeter routers; and

providing, to each of said plurality of security perimeter routers, a common discarding threshold, said discarding threshold defining a condition in which an incoming packet may be discarded at said security perimeter.

9. (previously presented) The method of claim 8, wherein said aggregating victim destination prefix lists and attack statistics associated with incoming packets comprises:

comparing measured attribute values to nominal traffic attribute values for packet traffic sent to a particular destination; and

identifying increases in said measured attribute values over said nominal traffic attribute values.

10. (previously presented) The method of claim 9, wherein said confirming said DDoS attack victim comprises determining if said identified increases for said measured attribute values exceed respective predetermined thresholds.

11. (previously presented) The method of claim 8, wherein said victim destination prefix list and attack statistics comprise at least one of packets per second (pps), bits per second (bps), flow counts, and flow rates of incoming packets.

12. (original) The method of claim 8, wherein said aggregating packet attribute distribution frequencies for incoming victim related packets comprises:

receiving packet attribute distribution frequencies from said plurality of security perimeter routers, said packet attribute distribution frequencies including incoming

813014-1

Serial No. 10/723,450
Page 33 of 39

packet attribute information comprising at least one of: IP protocol-type values, packet size, source/destination port numbers, source/destination IP prefixes, Time-to-Live (TTL) values, IP/TCP header length, TCP flag combinations, use IP fragmentation, and incorrect packet protocol checksums.

13. (original) The method of claim 8, wherein said aggregating packet attribute distribution frequencies for incoming victim related packets comprises:

receiving packet attribute distribution frequencies from said plurality of security perimeter routers, said packet attribute distribution frequencies including incoming packet attribute information comprising joint distribution of the fraction of packets having various combinations of Time-to-Live (TTL) values and source IP prefix, packet-size and protocol-type, and destination port number and protocol-type.

14. (original) The method of claim 13, wherein said receiving packet attribute distribution frequencies comprises receiving iceberg-style histograms comprising said incoming packet attribute information.

15. (original) The method of claim 8, wherein said generating common scorebooks comprises:

computing partial scores of different attributes; and
computing a weighted sum of said partial scores to yield a logarithmic function of conditional legitimate probability for each incoming packet.

16. (original) The method of claim 8, wherein said common discarding threshold comprises:

performing a load-shedding algorithm to determine a fraction (%_{PD}) of arriving suspicious packets required to be discarded; and
performing an inverse lookup on the aggregate CDF of scores.

17. (original) The method of claim 16, where at each of said plurality of security perimeter routers, said method further comprises:

813014-1

Serial No. 10/723,450
Page 34 of 39

determining whether a score of an incoming packet is less than or equal to said discarding threshold;

discarding said incoming packet in an instance said score is less than or equal to said discarding threshold; and

forwarding said incoming packet for routing to destination in an instance said score is greater than to said discarding threshold.

18. (previously presented) A method for selectively discarding packets at a security perimeter of a network during a distributed denial-of-service (DDoS) attack over [[a]] said network, comprising:

sending, from each of a plurality of routers forming said security perimeter, victim destination prefix list and attack statistics associated with incoming packets to a centralized controller adapted to confirm a victim of said DDoS attack;

sending, from each of said plurality of security perimeter routers, packet attribute distribution frequencies for incoming victim related packets;

receiving, at each of said plurality of security perimeter routers from said centralized controller, common scorebooks formed using aggregated packet attribute distribution frequencies and nominal traffic profiles;

sending, from each of said plurality of security perimeter routers, a local cumulative distribution function (CDF) of scores to said centralized controller; and

discarding, at each of said plurality of security perimeter routers, incoming packets based on a commonly distributed discarding threshold defined by said centralized controller.

19. (original) The method of claim 18, further including the step of classifying said incoming packets as being one of suspicious and non-suspicious packets based on a destination address of said incoming packet.

20. (original) The method of claim 19, wherein said local victim destination prefix list and attack statistics comprise at least one of packets per second (pps), bits per second (bps), flow counts, and flow rates of incoming packets.

813014-1

Serial No. 10/723,450
Page 35 of 39

21. (original) The method of claim 19, wherein said sending packet attribute distribution frequencies comprises monitoring packet attribute distribution frequencies including incoming packet attribute information comprising at least one of IP protocol-type values, packet size, source /destination port numbers, source/destination IP prefixes, Time-to-Live (TTL) values, IP/TCP header length, TCP flag combinations, use IP fragmentation, and incorrect packet protocol checksums.
22. (original) The method of claim 21, wherein said packet attribute distribution frequencies are sent in a form of iceberg-style histograms.
23. (original) The method of claim 20, wherein said sending a local cumulative distribution function (CDF) of scores comprises:
- determining a predetermined number of incoming packets to monitor;
 - for each incoming packet of said predetermined number of incoming packets:
 - determining attribute scores from said received scorebooks; and
 - locally aggregating said scores; and
 - forming said CDF from said aggregated scores associated with said predetermined number of incoming packets.
24. (original) The method of claim 19 wherein said commonly distributed discarding threshold comprises:
- a fraction ($\%_{PD}$) of arriving suspicious packets associated with an aggregated CDF from all of said routers.
25. (original) The method of claim 23, wherein said discarding said incoming packets comprises:
- determining whether a score of an incoming packet is less than or equal to said discarding threshold;

813014-I

Serial No. 10/723,450
Page 36 of 39

discarding said incoming packet in an instance said score is less than or equal to said discarding threshold; and

forwarding said incoming packet for routing to destination in an instance said score is greater than to said discarding threshold.

26. (previously presented) A centralized controller for determining packets to be dropped in regard to a potential distributed denial-of-service (DDoS) attack at a location within a packet network, said centralized controller comprising:

means for aggregating a plurality of packet attribute values respectively received from a plurality routers forming a security perimeter of a network to confirm said attack at said location, wherein said centralized controller is associated with said network;

means for computing an aggregate conditional probability measure for each packet entering said location based on selected attributes included within said packet from each location;

means for computing an aggregate cumulative distribution function (CDF) based on said computed aggregate conditional probability measures;

means for determining a drop threshold based on access to said cumulative probability function; and

means for sending said drop threshold to each of said plurality of security perimeter routers, wherein each of said plurality of security perimeter routers is adapted to pass through packets, that exceed said determined drop threshold, to said location.

27. (previously presented) A centralized controller for determining packets to be dropped in regard to a potential distributed denial-of-service (DDoS) attack at a location within a packet network, said centralized controller comprising:

means for aggregating, local victim destination prefix lists and attack statistics associated with incoming packets received from a plurality of routers of a network forming a security perimeter in said network, to confirm a victim of said DDoS attack, wherein said centralized controller is associated with said network ;

813014-I

Serial No. 10/723,450
Page 37 of 39

means for aggregating packet attribute distribution frequencies for incoming victim related packets received from said plurality of security perimeter routers;

means for generating common scorebooks from said aggregated packet attribute distribution frequencies and nominal traffic profiles;

means for aggregating local cumulative distribution function (CDF) of the local scores derived from said plurality of security perimeter routers; and

means for providing, to each of said plurality of security perimeter routers, a common discarding threshold, said discarding threshold defining a condition in which an incoming packet may be discarded at said security perimeter.

28. (previously presented) A network comprising:

a centralized controller for determining packets to be dropped in regard to a potential distributed denial-of-service (DDoS) attack at a location within a packet network; and

a plurality of security perimeter routers wherein each of said security perimeter routers comprises:

means for sending victim destination prefix lists and attack statistics associated with incoming packets to said centralized controller adapted to confirm a victim of said DDoS attack;

means for sending to said centralized controller packet attribute distribution frequencies for incoming victim related packets;

means for receiving, from said centralized controller, common scorebooks formed by aggregated packet attribute distribution frequencies and nominal traffic profiles;

means for sending a local cumulative distribution function (CDF) of scores to said centralized controller; and

means for discarding incoming packets based on a commonly distributed, to said plurality of security perimeter routers, discarding threshold defined by said centralized controller.

813014-1

Serial No. 10/723,450
Page 38 of 39

EVIDENCE APPENDIX

None

813014-1

Serial No. 10/723,450
Page 39 of 39

RELATED PROCEEDINGS APPENDIX

None

813014-1